



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/555,303	05/26/2000	Markus Feuser	PHD 99-096	3913

7590 06/16/2004
Philips Elcetronics North American Corp.
580 White Plains Rd.
Tarry town, NY 10591

EXAMINER

ARANI, TAGHI T

ART UNIT PAPER NUMBER

2131

DATE MAILED: 06/16/2004

9

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/555,303

Applicant(s)

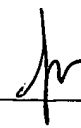
FEUSER, MARKUS

Examiner

Taghi T. Arani

Art Unit

2131



-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,4-6 and 9-11 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1, 4-6, 9-11 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. ____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____. |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152). |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date ____. | 6) <input type="checkbox"/> Other: ____. |

Art Unit: 2131

DETAILED ACTION

Claims 1-11 were pending for examination.

Claims 2-3, 7-8 are cancelled.

Claims 1, 4- 6, 9-11 are amended.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1 and 6 are rejected under 35 U.S.C. 101 because claims 1 and 6 recite “ a data processing device which includes an integrated circuit which executes useful arithmetic cryptographic operations” and “ the integrated circuit” is randomly switched” between different modes of operation” and “the different modes of operation.... including at least two calculation methods... which produce an identical result while using different arithmetic approaches”.

the language of the claims raises a question as to whether the claims are directed merely to an abstract idea that is not tied to a technological art, environment or machine which would result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 U.S.C. 101.

Claims 4-5, 9-11 are also rejected by virtue of their dependencies.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary

Art Unit: 2131

skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 4-6, 9-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over prior art of record, Griffin, III et al, and Sprunk and further in view of Ohki et al.

As per (amended) claims 1, 4, 6 and 9, Griffin is directed to a method for preventing compromise of secure data processing routines (i.e. a cryptographic operations) by a procedure known as a “clock attack”, see col. 1, lines 10-34. Griffin’s invention prevents clock attacks by providing a method that inhibits synchronization with externally generated instructions by preventing determination of the time of execution of a predetermined data processing routine in relation to occurrence of an externally observable event that precedes execution of the determined routine.

The method of Griffin includes step of randomly varying the duration between the occurrence of the externally observable event and the execution of the predetermined routine, see col. 1, lines 35-52.

Griffin’s invention implemented in a secure microprocessor executes a group of data processing routines (i.e. different modes of operation under random control), see col. 3, lines 1-36.

Griffin fails to teach a second clock signal derived from first clock signal under random control to be applied to the integrated circuit.

However, Sprunk discloses a secure microprocessor with reduced vulnerability to attack, see abstract, in which the secure microprocessor clock (i.e. first clock signal) is modulated (i.e. a second clock signal) in a substantially random fashion which eliminates the ability to predict the clock even if it is observable, see col. 1, lines 50-54.

Griffin-Sprunk fail to teach “two calculation methods which produce an identical result while using different arithmetic approaches”.

Art Unit: 2131

However, Ohki discloses an IC card chip wherein prior to executing an input data process of the IC card chip, the input data is transformed to thereby reduce the relation between the process data and the consumption current of the IC card chip, see abstract.

Ohki 's IC card includes a central processing unit for executing a data process in accordance with a program including one or more data process means each being a process instruction for giving an execution instruction to the central processing unit. The data processing means of Ohki comprises: a data transformed process means executing an operation OP1 on a transformed data H1 (which is the transformation of input data D1 by using a disturbance data Xi) and a data un-transforming processing means for executing an operation process OP2 which produces an identical value as the operation process OP1 for the input data D1. The teaching of Ohki suggests two calculation methods which produce an identical result while using different arithmetical approaches (recited in claims 1 and 6) and that a "dummy " operation (i.e. transforming input data using operation op1 on the disturbance data Xi) in which the IC card does not execute useful operations and un-transforming the transformed data (useful operation) wherein disturbance data (Xi) is rejected and not taken up in the results (recited in claims 4 and 9), see col. 4, lines 6-35, col. 6 line 10 through col 7, line 36.

It would have been obvious to one of ordinary skill in the art to employ secure microprocessor of Sprunk with clock signal modulation in secure data processing scheme of Griffin to preclude the observation of a clock signal and to render the observation of a portion of a clock signal useless for predicting the future operation, col. 1, lines 37-48 (Sprunk).

It would have been further obvious to one of ordinary skill in the art to modify Griffin's secure data processing routines to that of Ohki and Spunk to prevent both "clock attack" and

Art Unit: 2131

measuring and monitoring of the IC card consumption current (i.e. to prevent “Differential Power analysis”), see col. 1, lines 50-62 (Ohki et al.).

As per (amended) claims 5 and 10, Griffin teaches preventing the execution of a predetermined routine in response to a tamper detect counter, see abstract, see also col. 5, lines 12-18. that is, the integrated circuit does not execute arithmetic operations.

Allowable Subject Matter

Claim 11 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Response to Amendment

Applicant's arguments filed on 3/25/2004 regarding the rejection of the claims 1, 4-6,9-11 under 35 U.S.C. 103() have been fully considered but they are not persuasive.

As per Applicant's arguments relating to Ohki et al. reference, the Applicant argues that “Ohki generally describes equipment that performs a single calculation method, not an integrated circuit that is randomly switched between at least two calculation methods.”, page 5, 4th paragraph.

The Examiner disagrees. As addressed in the rejection of claims 1 and 6 above, Ohki's data processing equipment performs various processes (calculation methods) in transforming and un-transforming the input data by using a disturbance data Xi .

The Examiner further responds that the Ohki et al. is a secondary reference in a 103 type rejection used in combination with clock frequency modulation of Sprunk (for randomly switching between “at least two calculation methods”).

Art Unit: 2131

Action is Final

THIS ACTION IS FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion


Any inquiry concerning this communication or earlier communications from examiner should be directed to Taghi Arani, whose telephone number is (703) 305-4274. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The Fax numbers for the organization where this application is assigned is:

(703) 872-9306

Taghi Arani

Patent Examiner


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100